2011

Ore's theorem

Jarom Viehweg

Ore's Theorem

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Jarom Viehweg

June 2011

Ore's Theorem

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Jarom Viehweg

June 2011

Approved by:

[redacted]
Gary Griffing, Committee Chair

6/7/11
Date

[redacted]
Corey Dunn, Committee Member

[redacted]
Zahid Hasan, Committee Member

[redacted]
Peter Williams, Chair,
Department of Mathematics

Charles Stanton
Charles Stanton
Graduate Coordinator,
Department of Mathematics

Abstract

In elementary group theory, containment defines a partial order relation on the subgroups of a fixed group. This order relation is a *lattice* in the sense that it is a partially ordered set in which any two elements have a greatest lower bound and a least upper bound relative to the ordering. Lattices occur frequently in mathematics and form an extensive subject of study with a vast literature. While the subgroups of every group G always form a lattice, one might ask if every conceivable lattice is isomorphic to the subgroup lattice of some group. Furthermore, one might ask which kinds of lattice structures are isomorphic to which types of group structures. Such investigations are the content of this thesis, with the ultimate goal being to study the classical result in this direction discovered by O. Ore in 1938, as well as related theorems and corollaries.

Acknowledgements

I must begin by thanking Dr. Gary Griffing, who was integral in the development of my knowledge relating to the content of this thesis. I am grateful as well for his comments and suggestions throughout the writing the thesis itself and all of the time that he put into this effort. In addition, I would like to thank Dr. Corey Dunn and Dr. Zahid Hasan for serving on my thesis committee. I must also thank Paul Taylor for the use of his Commutative Diagrams LaTeX package and his helpful comments relating to its use. I also wish to thank the many teachers and professors I have had throughout my formal education. Their impact on my mathematical development has been profound and is appreciated.

Finally, I thank my family for their support in all of my educational endeavors over the years as well as for the countless other ways they have supported me throughout my life. Most especially, I thank my wife Kerri for the numerous personal sacrifices she has made. Without your selfless and tireless support, I would not have been able to balance all of my numerous obligations and acheive this personal goal of earning my master's degree in mathematics.

Table of Contents

List of Figures

Chapter 1

Introduction

In elementary group theory, containment defines a partial order relation on the subgroups of a fixed group. This order relation can be represented visually with a so-called *Hasse diagram* (for subgroups A and B, B is below A in the diagram if and only if $B \subseteq A$). Each of these Hasse diagrams forms a *lattice* in that it is a partially ordered set in which any two elements (subgroups in this case) have a meet, or greatest lower bound, and a join, or least upper bound.

For any group G, let $\mathrm{Sub}(G)$ denote the subgroup lattice of G as described above. $\mathrm{Sub}(G)$ can be formed in two primary ways. First, considering all subgroups of G, we can form the meet of any two subgroups by taking the intersection of those subgroups and the join of two subgroups by forming the subgroup generated by those subgroups. Second, we can create a lattice using only the normal subgroups of G where the meet is again the intersection of any two subgroups; however, in this case the join of two subgroups is created by taking the product of the two normal subgroups. In both of these cases, the ordering is by inclusion. Note that for commutative groups, these two methods coincide. That is, as every subgroup of a commutative group is normal, the product of any two subgroups equals the subgroup generated by them.

As we can form a lattice from every group, one might ask the converse, that is, if every conceivable lattice is isomorphic to the subgroup lattice of some group. Furthermore, one might ask which kinds of lattice structures are isomorphic to which types of group structures. In so doing, we can investigate a property X possessed by a class of groups and a corresponding property Y possessed by a class of lattices so as to be able

to say: "A group G satisfies property X if and only if its corresponding subgroup lattice satisfies property Y." Such investigations are the content of this thesis, with the ultimate goal being to study the classical result in this direction discovered by O. Ore in 1938, as well as related theorems and corollaries.

Chapter 2

Lattices

2.1 Basic Definitions and Examples

We begin by introducing the formal definition of a lattice, its meet and join, and some examples of lattices. Before we define a lattice, however, we must understand the underlying structure of lattices, namely partially ordered sets. Therefore, we will begin with the following definition:

Definition 2.1. Let P be a set equipped with a binary relation $\leq$, sometimes denoted by $\langle P; \leq \rangle$. Then P is considered to be a *partially ordered set* (or *poset*) if $\leq$ satisifies the following three axioms for all $a, b, c \in P$:

1. $a \leq a$ (Reflexive property)
2. $a \leq b$ and $b \leq a$ implies $a = b$ (Anti-symmetric property)
3. $a \leq b$ and $b \leq c$ implies $a \leq c$ (Transitive property)

Furthermore, $\leq$ itself is said to be a *partial ordering* (or *ordering*) of P.

As we move forward, it will be useful to define the dual of a partially ordered set and to prove the duality principle. This will be especially useful as when we discuss distributive lattices as well as in order to prove distributivity (see Definition 2.24).

Proposition 2.2. *Let $\langle P; \leq \rangle$ be a poset. Then $\langle P; \geq \rangle$ is also a poset.*

Proof. First, we note that the binary relation $\geq$ is well-defined: $a \geq b$ simply means $b \leq a$. Then for elements $a, b, c \in P$ where $\leq$ is a partial ordering, each of the three partial order axioms are satisfied for $\geq$, meaning $\geq$ is a partial ordering as well, and $\langle P; \geq \rangle$ is a poset. □

Definition 2.3. Given $\langle P; \leq \rangle$, the poset $\langle P; \geq \rangle$ is called the *dual* of P and is denoted by P^{∂}.

Proposition 2.4 (The Duality Principle)**.** *If an expression Φ involving ordering is true in all posets, then Φ^{∂} is also true in all posets.*

Proof. It is clear that Φ holds in $\langle P; \leq \rangle$ if and only if Φ^{∂} holds in $\langle P; \geq \rangle$. □

Definition 2.5. Given a poset P, the *meet* of two elements $a, b \in P$ is the greatest lower bound, denoted $a \wedge b$. That is, $a \wedge b$ is the (necessarily) unique element such that

1. $a \wedge b \leq a$ and $a \wedge b \leq b$.
2. If there exists an element $c \in P$ such that $c \leq a$ and $c \leq b$, then $c \leq a \wedge b$.

Definition 2.6. Given a poset P, the *join* of two elements $a, b \in P$ is the least upper bound, denoted $a \vee b$. That is, $a \vee b$ is the (necessarily) unique element such that

1. $a \leq a \vee b$ and $b \leq a \vee b$.
2. If there exists an element $c \in P$ such that $a \leq c$ and $b \leq c$, then $a \vee b \leq c$.

Note that meet and join are duals of each other as described in Definition 2.3. This fact will be useful as we move forward, particularly with regards to distributive lattices (see Definition 2.24).

Proposition 2.7. *Whenever meet and join are defined as above, $a \wedge b = b \wedge a$ and $a \vee b = b \vee a$ for all $a, b \in P$.*

Proof. Definitions 2.5 and 2.6 imply that meet and join of two elements are unique. Therefore, since $b \wedge a$ is the meet of a and b, $b \wedge a = a \wedge b$ by uniqueness of meet. We also find that $b \vee a = a \vee b$ by a similar argument. □

With the above definitions in hand, we are ready to formally define the concept of a lattice.

Definition 2.8. A *lattice* L is a partially ordered set in which every pair of elements has a meet and a join. Furthermore, a subset of a lattice L is called a *sublattice* of L if it is itself a lattice with respect to the join and meet on L.

The following are examples of lattices:

Example 2.9. Consider the power set of S, i.e., the set of all subsets of a given set S, denoted $\mathcal{P}(S)$. $\mathcal{P}(S)$ forms a lattice where ordering is containment, meet is intersection, and join is union (See Figure 2.1).

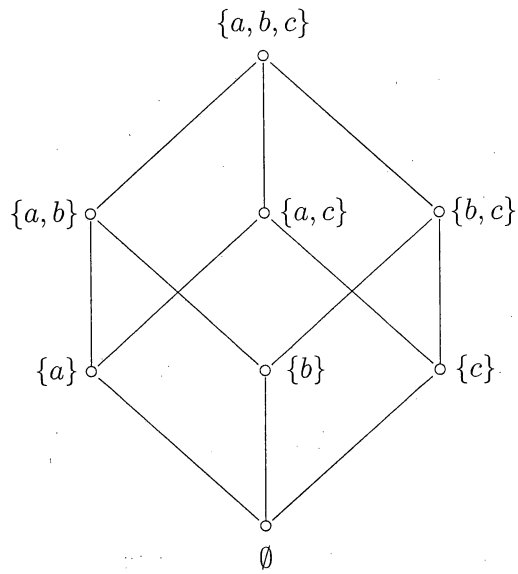


Figure 2.1: Power set of $\{a, b, c\}$

Example 2.10. Any (open or closed) interval of real numbers, rational numbers, or integers forms a lattice with the usual ordering where meet and join are the binary operations of min and max, respectively. Specifically, these intervals form lattice chains (see Definintion 2.14 and Figure 2.2 below).

Definition 2.11. We say a lattice L has a *top* element $\top$ if $a \leq \top$ for all $a \in L$. Similarly, we say L has a *bottom* element $\bot$ if $\bot \leq a$ for all $a \in L$.

Example 2.12. The lattice formed by the power set $\mathcal{P}(S)$ has S as its top and the empty set as its bottom (See Figure 2.1).

Example 2.13. The closed interval of real numbers $[0, 1]$ forms a lattice as described in the preceding example. It has $\bot = 0$ and $\top = 1$. The open interval of reals $(0, 1)$ has neither a top nor a bottom. The real interval $[0, 1)$ has $\bot = 0$ but no top, and the interval $(0, 1]$ has $\top = 1$ but no bottom.

In addition to those examples we have presented, two common types of posets that are used to form lattices are *chains* and *antichains*, defined and pictured below.

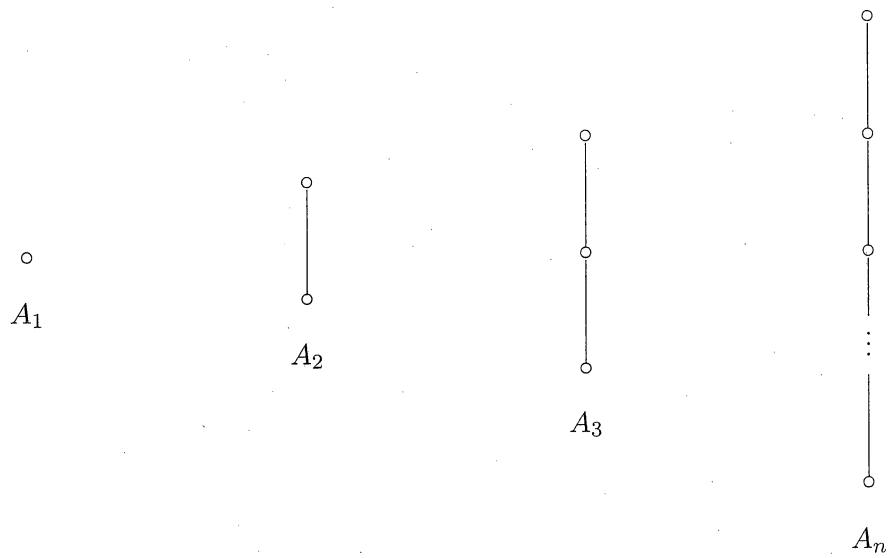


Figure 2.2: Lattice chains

Definition 2.14. A *chain* is a poset P in which for two elements x and y in the set, either $x \leq y$ or $y \leq x$. That is, all elements of P are said to be *comparable.*

It is simple to verify that chains form not only posets, but lattices as well. We can see that the chain A_1 is the trivial lattice, A_2 is the chain with exactly two comparable elements, and in general, A_n is the chain with exactly n comparable elements. In general, a lattice (including chains) need not be finite. Consider the following example.

Example 2.15. The converging sequence of rational numbers $1, 1/2, 1/4, 1/8, \ldots$ with the usual ordering and the binary operations of min and max as meet and join is an infinite descending chain. This lattice has as its top $\top = 1$, but does not have a bottom. Note that although 0 is the greatest lower bound of this set, it is not an element of the lattice, and thus cannot be the bottom of the lattice. The sequence of integers $1, 2, 4, 8, \ldots$ is an infinite ascending chain.

Another important class of posets that can be used to form lattices are antichains, defined below.

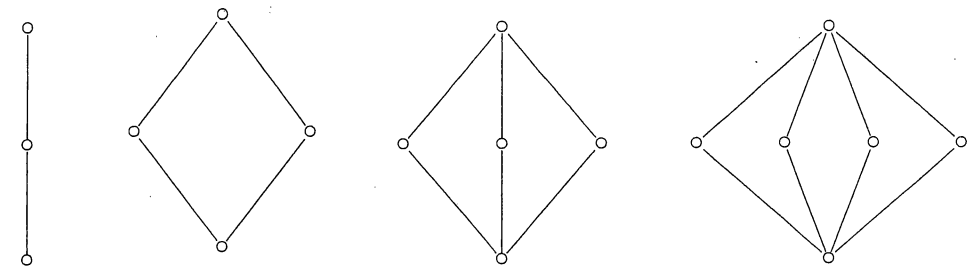


Figure 2.3: Lattice antichains

Definition 2.16. An *antichain* is a poset P in which for two elements x and y, $x \leq y$ implies $x = y$. If $x \neq y$, we say that x and y are *parallel*, i.e., $x \parallel y$.

An antichain with more than one element does not form a lattice as no two distinct elements have a meet or join. However, if we adjoin a top and bottom to an antichain, it does become a lattice. (By adjoin, we mean define a new ordering in which the elements of the antichain are still incomparable, but the top is greater than or equal to every element in the antichain and the bottom is less than or equal to every element in the antichain.) We note that that the lattice M_2 contains the antichain with exactly two parallel elements (and a top and bottom), M_3 contains the antichain with exactly three parallel elements, and M_n contains the antichain with exactly n parallel elements. We will refer to these lattices as *antichain lattices*.

Although chains and antichains are important classes of lattices, not to mention the many other types of lattices worthy of study, our main focus is to study lattices and their association with groups as mentioned in the Introduction.

Definition 2.17. Let $\mathrm{Sub}(G)$ denote the poset formed from the collection of all subgroups of a fixed group G where ordering is given by containment.

Proposition 2.18. *Let G be a group and let X be any subset of G. Write $\langle X\rangle = \bigcap_\Gamma C$ where Γ is the collection of subgroups $C \subseteq G$ that contain X. Then $\langle X\rangle$ is the smallest (contained in every other) subgroup of G containing X.*

Proof. It is well-known that the intersection of subgroups is a subgroup. The intersection is contained in every $C \in \Gamma$, therefore it is the smallest. □

Definition 2.19. We will call $\langle X\rangle$ in the proposition above the *subgroup generated by* X.

Proposition 2.20. *The meet of two subgroups in $Sub(G)$ is the intersection of those subgroups, and the join of two subgroups is the subgroup generated by their union. As such, $Sub(G)$ is a lattice with $\top = G$ and $\bot = \{e\}$.*

Proof. It is clear from the definition of the intersection of two subgroups that the meet in $\mathrm{Sub}(G)$ is in fact the intersection. (Thus, we can say that $\mathrm{Sub}(G)$ is a meet-sublattice of $\mathcal{P}(S)$.) However, the union of subgroups is not typically itself a subgroup, and therefore cannot be the join.

Claim. *In $Sub(G)$, the join of two subgroups $A, B \subseteq G$ is given by the subgroup generated by A and B.*

Let $X = A \cup B$. Then $\langle X\rangle = \bigcap_\Gamma C$ where Γ is the collection of subgroups $C \subseteq G$ that contain both A and B. It is clear that $A \subseteq \langle X\rangle$ and $B \subseteq \langle X\rangle$. Moreover, if we find a subgroup D such that $A \subseteq D$ and $B \subseteq D$, then $D \in \Gamma$, and $\langle X\rangle \subseteq D$. As such, $\langle X\rangle$ fulfills the exact criteria for join listed in Definition 2.6. Finally, because $\mathrm{Sub}(G)$ is a poset with binary meets and joins, $\mathrm{Sub}(G)$ is a lattice. □

Example 2.21. We will now proceed to completely describe $\mathrm{Sub}(\mathbb{Z})$. Note that $\mathbb{Z}$ and all of its subgroups are cyclic. We know $\langle b\rangle \subseteq \langle a\rangle$ if and only if $a \mid b$.

Claim. $\langle a\rangle \wedge \langle b\rangle = \langle c\rangle$ *where* $c = \mathrm{lcm}(a, b)$ *and* $\langle a\rangle \vee \langle b\rangle = \langle d\rangle$ *where* $d = \gcd(a, b)$.

By the properties of meet, $\langle c\rangle$ satisfies

1. $\langle c\rangle \subseteq \langle a\rangle$ and $\langle c\rangle \subseteq \langle b\rangle$.

2. If $\langle m \rangle \subseteq \langle a \rangle$ and $\langle m \rangle \subseteq \langle b \rangle$, then $\langle m \rangle \subseteq \langle c \rangle$.

Therefore, by the ordering c satisfies

1. $a \mid c$ and $b \mid c$.

2. $a \mid m$ and $b \mid m$ implies $c \mid m$.

As the above properties are precisely the definition of least common multiple, we have $c = \text{lcm}(a, b)$. By similar analysis, we find that $\langle a \rangle \vee \langle b \rangle = \langle d \rangle$ where $d = \gcd(a, b)$.

This is also true for $\mathbb{Z}_n$ under calculations modulo n. The example below gives details of this calculation for $\mathbb{Z}_{36}$, whose subgroup lattice is pictured in Figure 2.4.

Example 2.22. The following are some calculations for meet and join in $\text{Sub}(\mathbb{Z}_{36})$:

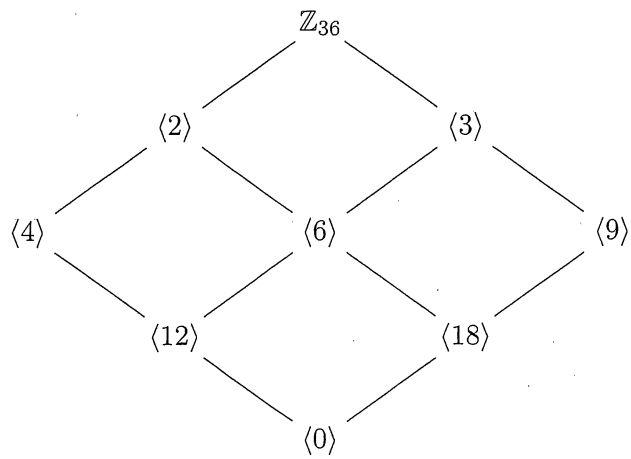


Figure 2.4: $\text{Sub}(\mathbb{Z}_{36})$

1. $\langle 2 \rangle \vee \langle 3 \rangle = \mathbb{Z}_{36}$ whereas $\langle 2 \rangle \wedge \langle 3 \rangle = \langle 6 \rangle$.

2. $\langle 4 \rangle \vee \langle 9 \rangle = \mathbb{Z}_{36}$ and $\langle 4 \rangle \wedge \langle 9 \rangle = \langle 0 \rangle$.

3. $\langle 3 \rangle \vee \langle 12 \rangle = \langle 3 \rangle$ and $\langle 3 \rangle \wedge \langle 12 \rangle = \langle 12 \rangle$.

4. $\langle 9 \rangle \vee \langle 12 \rangle = \langle 3 \rangle$ and $\langle 9 \rangle \wedge \langle 12 \rangle = \langle 0 \rangle$.

In the sections that follow, it will become important for us to talk about what it means for a lattice L to be isomorphic to the subgroup lattice $\mathrm{Sub}(G)$ for some group G. Hence, we will define a lattice isomorphism below.

Definition 2.23. Let L and K be lattices. A map $\phi : L \to K$ is a *lattice homomorphism* if it preserves meets and joins, that is, $\phi(a \wedge b) = \phi(a) \wedge \phi(b)$ and $\phi(a \vee b) = \phi(a) \vee \phi(b)$ for all $a, b \in L$. If ϕ is bijective, we call ϕ a *lattice isomorphism.*

Two lattices L and K are considered to be *isomorphic*, denoted by $L \cong K$, if there exists a lattice isomorphism $\phi : L \to K$.

2.2 Distributive Lattices

Definition 2.24. A lattice L is called *distributive* if for all $a, b, c \in L$:

1. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, and
2. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

An important consequence of the Principle of Duality is that statement 1 of Definition 2.24 holds for every poset if and only if statement 2 holds for every poset. Thus, when we verify the distributive property we need only verify one of these two statements. In the same vein, part of the distributive law automatically holds for every lattice as shown below.

Proposition 2.25. *Let L be a lattice and let $a, b, c \in L$. Then*

1. $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$, *and*
2. $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

Proof. 1. To show $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ we will first show $a \vee (b \wedge c) \leq (a \vee b)$ and $a \vee (b \wedge c) \leq (a \vee c)$. But it is clear by Definition 2.5 that $(b \wedge c) \leq b$ and $(b \wedge c) \leq c$, and so $a \vee (b \wedge c) \leq (a \vee b)$ and $a \vee (b \wedge c) \leq (a \vee c)$. But $(a \vee b) \wedge (a \vee c)$ is the greatest lower bound of $a \vee b$ and $a \vee c$ by definition, and so $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

2. We use a similar approach to that used in part 1 above. To show $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$, we need only show $(a \wedge b) \vee (a \wedge c) \leq a$ and $(a \wedge b) \vee (a \wedge c) \leq (b \vee c)$. By

definition, $a \wedge b \leq a$ and $a \wedge c \leq a$. But $(a \wedge b) \vee (a \wedge c)$ is the least upper bound of $a \wedge b$ and $a \wedge c$, so $(a \wedge b) \vee (a \wedge c) \leq a$. Additionally, $a \wedge b \leq b$ and $a \wedge c \leq c$, respectively. But then $(a \wedge b) \vee (a \wedge c)$ is below both b and c. Since $b \wedge c$ is the greatest lower bound of b and c, $(a \wedge b) \vee (a \wedge c) \leq (b \wedge c)$. Thus, $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$. □

This proposition greatly simplifies our work in proving that a lattice is distributive. It enables us to prove equality by simply showing $(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge c)$ or $a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$.

Now, we will look at some examples of distributive and non-distributive lattices.

Example 2.26. It is easy to show that the power set $\mathcal{P}(S)$ is distributive for every set S.

For a fixed group G, we note that when regarded as a poset, $\mathrm{Sub}(G)$ is a subposet of $\mathcal{P}(G)$. However, $\mathrm{Sub}(G)$ is not a sublattice of $\mathcal{P}(G)$ as the joins are different. Additionally, while $\mathcal{P}(S)$ is always distributive, $\mathrm{Sub}(G)$ is only sometimes distributive as illustrated in the two examples below.

Example 2.27. For $G = \mathbb{Z}_{36}$, $\mathrm{Sub}(G)$ is distributive.

This can be verified directly by repeatedly replacing every combination of three elements in $\mathrm{Sub}(\mathbb{Z}_{36})$ into statement 1 of Definition 2.24. For example, we verify the left-hand side of statement 1 of Definition 2.24 using the subgroups $\langle 3 \rangle, \langle 4 \rangle$, and $\langle 18 \rangle$. Then we have $\langle 3 \rangle \vee (\langle 4 \rangle \wedge \langle 18 \rangle) = \langle 3 \rangle \vee \langle 0 \rangle = \langle 3 \rangle$. Checking the right-hand side, $(\langle 3 \rangle \vee \langle 4 \rangle) \wedge (\langle 3 \rangle \vee \langle 18 \rangle) = \mathbb{Z}_{36} \wedge \langle 3 \rangle = \langle 3 \rangle$.

Clearly, this would be a painstaking process if it were continued for all combinations of the elements in $\mathrm{Sub}(\mathbb{Z}_{36})$ However, this fact follows readily from Ore's Theorem (Theorem 4.6).

Example 2.28. For $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathrm{Sub}(G)$ is not distributive.

Let $A = \langle (0,1) \rangle, B = \langle (1,1) \rangle$ and $C = \langle (1,0) \rangle$ be the three non-trivial cyclic subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$ (See Figure 2.5). Considering the left-hand side of statement 1 of Definition 2.24, $A \vee (B \wedge C) = A \vee \{e\} = A$. On the right-hand side, however, we get $(A \vee B) \wedge (A \vee C) = (\mathbb{Z}_2 \times \mathbb{Z}_2) \wedge (\mathbb{Z}_2 \times \mathbb{Z}_2) = \mathbb{Z}_2 \times \mathbb{Z}_2$, and so $\mathrm{Sub}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is not distributive.

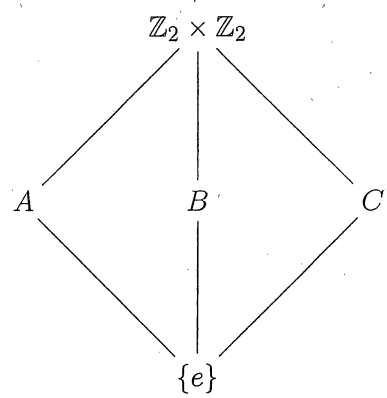


Figure 2.5: $\mathrm{Sub}(\mathbb{Z}_2 \times \mathbb{Z}_2)$

2.3 Lattices and Groups

Thus far, we have begun to see the correspondence between lattices and groups. At this point, one may begin to wonder to what extent lattices and groups are related. Specifically, we might ask if every lattice is isomorphic to $\mathrm{Sub}(G)$ for some group G. We begin by considering chains. It is obvious that the trivial chain A_1 is simply formed from the trivial group, $G = \{e\}$. But what about A_2, A_3, etc.? We must begin by considering the structure of such lattices and try to find a group whose subgroup lattice exhibits the same structure.

Considering A_2, we must find a group whose only proper subgroup is the trivial subgroup. Indeed, one such example is the group $\mathbb{Z}_p$ for any prime p. As we proceed to seek out a group whose subgroup structure is equivalent to that of A_3, we might try to construct a group that has $\mathbb{Z}_p$ as its only non-trivial proper subgroup. We find that $\mathbb{Z}_{p^2}$ is such a group, and A_3 is indeed its subgroup lattice. Now a clear pattern has emerged, and if we continue this pattern inductively, we find that $\mathrm{Sub}(\mathbb{Z}_{p^{n-1}}) \cong A_n$. We have thus found a class of groups that capture all finite chains.

But what about other classes of lattices? For example, can we find a group G such that $\mathrm{Sub}(G) \cong M_n$, for example? The lattice $\mathrm{Sub}(\mathbb{Z}_{p^2}) \cong A_3 \cong M_1$ as shown above, and we have already seen that $\mathrm{Sub}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong M_3$ (Compare Figures 2.3 and 2.5). It is also relatively simple to find (distinct) groups whose subgroup lattices are isomorphic to M_2 as well as M_4 as shown in the following two Propositions.

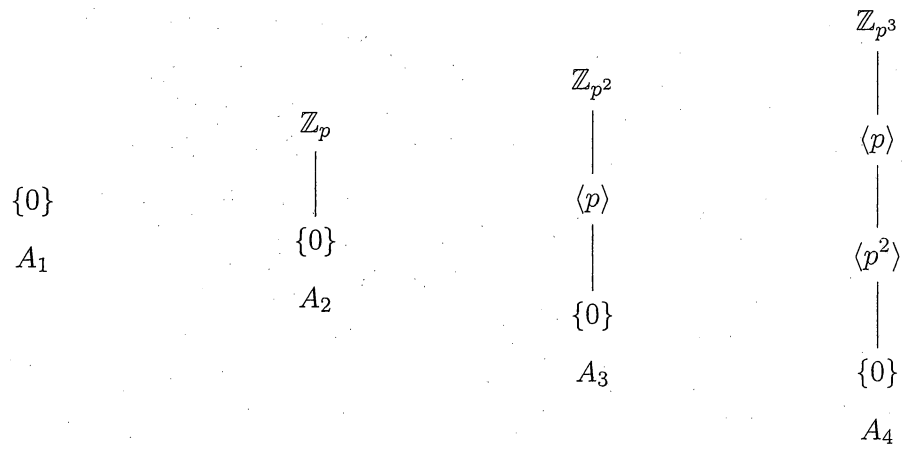


Figure 2.6: Lattice chains and subgroup lattices

Proposition 2.29. *$Sub(\mathbb{Z}_{pq}) \cong M_2$ where p and q are distict primes.*

Proof. We will analyze the subgroup structure of $\mathbb{Z}_{pq}$ using the Fundamental Theorem of Cyclic Groups (Theorem 3.1). Since $|Z_{pq}| = pq$, the Fundamental Theorem of Cyclic Groups guarantees that for each positive divisor of pq there is exactly one subgroup of G. All divisors of pq are pq, p, q and 1, and thus $\mathbb{Z}_{pq}$ has exactly 4 distinct subgroups. It is clear that $\top = \mathbb{Z}_{pq}$ and that $\bot = \{0\}$. Because $\gcd(p, q) = 1$, we conclude that the two intermediate subgroups of orders p and q have no elements in common besides the identity, and are thus parallel. Therefore, $\mathrm{Sub}(\mathbb{Z}_{pq})$ (pictured in Figure 2.7) has the same structure as M_2, and so $\mathrm{Sub}(\mathbb{Z}_{pq}) \cong M_2$. □

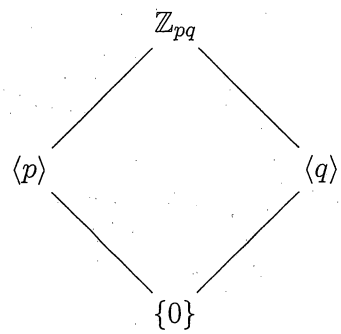


Figure 2.7: $\mathrm{Sub}(\mathbb{Z}_{pq})$

Proposition 2.30. *$Sub(S_3) \cong M_4$.*

Proof. Recall that S_3 has 6 elements, namely $\{e, (123), (132), (12), (13), (23)\}$. The subgroups of S_3 are S_3 itself, $\langle(123)\rangle, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$, and $\{e\}$. Each of the subgroups generated by the two-cycles have order 2, while $\langle(123)\rangle = \{e, (123), (132)\}$. Thus, these 4 subgroups are incomparable, and each is contained in S_3 and contains $\{e\}$. Therefore, we see that $\text{Sub}(S_3) \cong M_4$. Note that $(ab)(bc) = (abc)$, $(abc)(ab) = (ac)$, and $(ab)(abc) = (bc)$, and thus $\langle(ab)\rangle \vee \langle(bc)\rangle = S_3 = \langle(ab)\rangle \vee \langle(abc)\rangle$. □

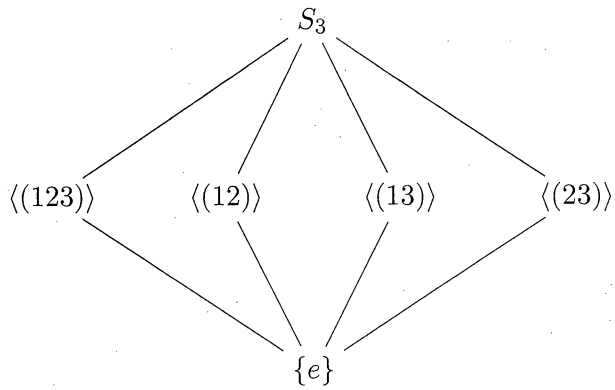


Figure 2.8: $\text{Sub}(S_3)$

We have now managed to capture M_n for $1 \leq n \leq 4$; however, we have not been able to do so as neatly as we did for A_n. Although we were able to find a single class of groups G such that $\text{Sub}(G) \cong A_n$, each of the groups whose subgroup lattice is isomorphic to M_n have been distinct types. While we might try to extend those results we already have for M_n as we did with A_n, we will find very quickly that such extensions will not work. (S_4, for example, has 30 subgroups, and S_5 has over 100! [Gallian, 96]). Indeed, finding groups whose subgroup lattices are isomorphic to M_n becomes a much more difficult question to answer in general, and leads us to question whether it is possible to find a group G such that $\text{Sub}(G) \cong L$ for every lattice L. It turns out that the answer to this question is no. In order to show this, we will consider the pentagonal lattice N_5, represented in Figure 2.9.

Proposition 2.31. *There is no group G that satisfies $Sub(G) \cong N_5$.*

Proof. We proceed by contradiction. We will assume that there is some group G with a subgroup lattice structure isomorphic to N_5, that is, assume G has three non trivial subgroups, A, B and C, which along with G and $\{e\}$ make up all the subgroups of G. Further assume that the subgroups have containment relations $\{e\} \subseteq A \subseteq G$ and $\{e\} \subseteq C \subseteq B \subseteq G$, but that no part of A is contained in B or C, and visa versa, besides the identity e.

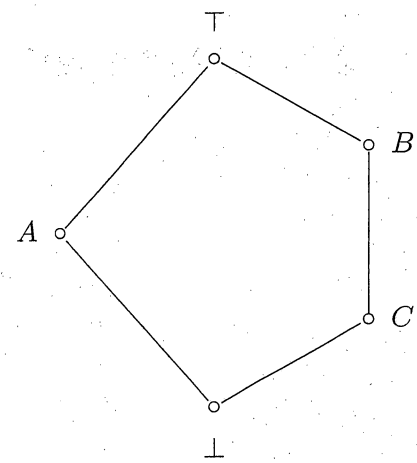


Figure 2.9: N_5

Claim. *G is not infinite cyclic.*

If G is infinite cyclic, then there exists an element a of infinite order such that $\langle a \rangle = G$. Furthermore, if a has infinite order, there is no nonzero integer n such that a^n is the identity. If we suppose $a^i = a^j$, then $a^i a^{-j} = a^j a^{-j}$, and so $a^{i-j} = e$. This implies that $i - j = 0$, that is, $i = j$. Therefore, the subgroups $\langle a^j \rangle$ for $j \geq 0$ are all distinct. However, G has exactly 5 distinct subgroups, and so this contradicts the assumed structure of G. Therefore, G is not infinite cyclic.

Claim. *G is finite cyclic.*

Consider the subgroup A. It contains some non-identity element a and $\langle a \rangle$ forms a subgroup. However, as the only proper subgroup of A is the bottom, $\langle a \rangle = A$, and as

such, A is cyclic. By Claim 1, $|A| < \infty$. Now, by the Fundamental Theorem of Cyclic Groups (see Theorem 3.1) we can determine the order of A. The theorem states that A must have exactly one subgroup of order equal to each of its divisors. However, the bottom has only one element, and thus has order 1. Therefore, as 1 is the only divisor of $|A|$ (besides itself), A must have prime order p. Similarly, the subgroup C is cyclic, i.e., $\langle c \rangle = C$ for some c in C, and must have prime order q.

Now, consider the subgroup B. Since $C \subseteq B, c \in B$. More specifically, however, $C \subsetneq B$, so B must contain another element $b \in B \setminus C$. Now, as $\langle b \rangle \nsubseteq C$ and there are no subgroups contained in C besides the bottom, $\langle b \rangle = B$, implying that B is cyclic. Moreover, because C is a subgroup of B, $|C|$ divides $|B|$ by Lagrange. Suppose $|B| = mq$ for some $m \geq 1$. Recall that B already has one subgroup of order q. By the Fundamental Theorem of Cyclic Groups, B must have exactly one subgroup of order every divisor of m. However, B contains no other subgroups besides C and the bottom. Additionally, $|B| \neq |C|$ as the orders must be distinct, so the only other possible choice is $m = q$, that is, $|B| = q^2$.

Finally, we consider G. Either $G = A \cup B$ or $A \cup B \subsetneq G$. Since G is closed, we have that $ab \in G$. However, ab cannot equal e because $ab = e$ implies that a and b are inverses of each other. If that were so, then $b \in A$ and $a \in B$, respectively, which would contradict the assumed lattice structure of $\mathrm{Sub}(G)$. But $a \notin B$ and $b \notin A$, so $ab \notin A$ and $ab \notin B$. Therefore, $G \neq A \cup B$. Thus, we can find an element g such that $g \in G \setminus (A \cup B)$. But then $\langle g \rangle$ forms a subgroup of G. Because $g \notin A \cup B$, $g \notin A$ and $g \notin B$ or any of their subgroups. Thus, $\langle g \rangle = G$, and therefore G is cyclic.

Now, because G is finite, the orders of A, B and C, which are p, q^2 and q respectively, must divide the order of G by Lagrange. Then $|G| = mpq^2$ for some $m \geq 1$. But then $G = \langle g \rangle$ would have *at least* one more subgroup of order pq distinct from A, B and C by the Fundamental Theorem of Cyclic Groups. Therefore, G cannot be a group with the assumed subgroup lattice structure. □

Having proven the preceding result, we now know definitively that not every lattice is isomorphic to the subgroup lattice of some group. So, while it is true that there exists a lattice that is isomorphic to $\mathrm{Sub}(G)$ for every group G, namely $\mathrm{Sub}(G)$ itself, the converse is not true for every lattice. That is, by Proposition 2.31, not everly lattice arises as $\mathrm{Sub}(G)$ for some group G. Although not every lattice is isomorphic to $\mathrm{Sub}(G)$

of some group G, in 1946 Ph. Whitman was able to find a direct correspondence between groups and sublattices as follows.

Theorem 2.32 (Ph. Whitman, 1946). *Every lattice is isomorphic to a sublattice of $Sub(G)$ for some group G.*

Proof. A proof of this result is not only difficult, but far beyond the scope of this project. However, an interested reader can find one proof of this theorem in Gratzer, p. 196. □

We wonder if we can find a certain class of lattices that are always isomorphic to $\mathrm{Sub}(G)$ for some group G. For example, by Proposition 2.31, we might ask if every distributive lattice can be found to be isomorphic to $\mathrm{Sub}(G)$ for some group G. Or, can we show that if G has a specific group structure, $\mathrm{Sub}(G)$ will always exhibit some specific lattice structure? In 1938, O. Ore found one satisfactory answer to this question. Specifically, he showed that the underlying group G is locally cyclic if and only if the corresponding subgroup lattice $\mathrm{Sub}(G)$ is distributive (See Theorem 4.6). In order to prove this result, however, we will need to use a considerable amount of group theory.

Chapter 3

The Structure of Finite and Finitely Generated Abelian Groups

As Ore's Theorem truly is a bridge between lattice theory and group theory, its proof is steeped in the structure of groups in addition to lattice theory. Because to this, we will need to discuss fundamental results about the structure of finite abelian groups and finitely generated abelian groups as well as associated results. The proof of Ore's Theorem also relies the Second Isomorphism Theorem of Groups, which is presented hereafter. Additionally, the Fundamental Theorem of Cyclic Groups was referenced numerous times as we discussed the structure of cyclic groups and their associated subgroup lattices. Its statement and proof are given subsequently.

3.1 Basic Group Theory

In this section, groups are considered abstract and are written multiplicatively.

Theorem 3.1 (Fundamental Theorem of Cyclic Groups). *Consider the cyclic group* $G = \langle a \rangle$. *Then*

1. *Every subgroup of* G *is cyclic.*
2. *If* $|G| = n$, *the order of any subgroup of* G *divides* n.

3. *For each positive divisor k of $n = |G|$ there is exactly one subgroup of G, namely $\langle a^{n/k} \rangle$.*

Proof. 1. Let H be a subgroup of G. We will consider the set $S = \{k \in \mathbb{Z}^+ | a^k \in H\}$. Suppose $H \neq \{e\}$. Then a^n is an element of H, S is non-empty, and by the Well-Ordering Principle, S has a least element, say t. We will show that $H = \langle a^t \rangle$ by double-inclusion. First, since $a^t \in H$, $H \supseteq \langle a^t \rangle$ by closure. Second, we consider $h \in H$. We note that $h = a^k$ for some $k \in \mathbb{Z}^+$. By the Division Algorithm, we can find integers q and r such that $k = tq + r$ where $0 \leq r < k$. Then $a^k = a^{tq+r} = a^{tq}a^r$. This implies $a^r \in H$. Now, as t is the least element of S, $r = 0$, and so $h = a^{tq} \in \langle a^t \rangle$. So $H \subseteq \langle a^t \rangle$. Therefore, $H = \langle a^t \rangle$.

2. This follows from Lagrange.

3. To show there is exactly one subgroup for each divisor of n, we suppose by contradiction that there are two subgroups of G of order k, namely H and K. Suppose $H = \langle a^t \rangle$ and $K = \langle a^s \rangle$ where s and t are the least positive integers such that $a^t \in H$ and $a^s \in K$. Then $t|m$ and $s|m$ for all m where $a^m \in H$ and $a^m \in K$. Because $a^n = e \in H \cap K$, t and s must divide n as well. Now, as n is the least positive integer such that $a^n = e$ and k is the least such that $(a^t)^k = e$, $a^{tk} = a^n = a^{t\frac{n}{t}}$, so $k = \frac{n}{t}$. Similarly, $k = \frac{n}{s}$, implying $\frac{n}{t} = \frac{n}{s}$, so $t = s$. Thus, $H = K = \langle a^t \rangle$, and as $t = \frac{n}{k}$, $\langle a^t \rangle = \langle a^{n/k} \rangle$.

□

Definition 3.2. If G is a group and H and K are subsets of G, $HK = \{hk \mid h \in H, k \in K\}$.

Note, HK is also a subset of G. In fact, sometimes, HK is more than a subset; it can form a subgroup, as shown in the following.

Theorem 3.3 (Second Isomorphism Theorem of Groups)**.** *Let H and K be subgroups of a group G where K is a normal subgroup of G, denoted by $K \trianglelefteq G$. Then HK is a subgroup of G and $H/(H \cap K) \cong HK/K$.*

Proof. We first show that HK is a subgroup of G. We note that HK contains the identity since both H and K are subgroups of G. We proceed by the two-step subgroup

test. First, we show that HK is closed. We take $a = h_1k_1$ and $b = h_2k_2$. Then we must show that $ab = h_1k_1h_2k_2 \in HK$. But then $ab = h_1h_2h_2^{-1}k_1h_2k_2$ as $e \in HK$. But $h_2^{-1}k_1h_2 \in GKG^{-1} \subseteq K$ since K is a normal subgroup of G, i.e., $h_2^{-1}k_1h_2 = k_3$, and $h_1h_2k_3k_2 \in HK$, so HK is closed. Second, we must show that $a^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in HK$. But $k^{-1}h^{-1} = h^{-1}hk^{-1}h^{-1}$. But as $hk^{-1}h^{-1} \in GKG^{-1}, a^{-1} = h^{-1}k' \in HK$. Therefore, HK is a subgroup of G.

For the second part of the theorem, consider the homomorphism ϕ: $H \to HK/K$ that takes h to hK. We note that ϕ is onto since given an $hkK \in HK/K$, we find that h maps to $hK = hkK$.

Now, we take $h \in \ker\phi$. Then $\phi(h) = 1K = K$. But as $\phi(h) = hK$, we have $hK = K$, which is true if and only if $h \in K$. Thus, $\ker\phi = H \cap K$. Hence, applying the First Isomorphism Theorem of Groups, we have that

$$H/(H \cap K) \cong HK/K.$$

□

3.2 Finite Abelian Groups

The goal of this section is to determine the structure of finite abelian groups. Theorem 3.12 and Theorem 3.16 together state that a finite abelian group breaks down into a direct sum of cyclic p-groups (*direct sum* and *p-group* are defined below; see Definitions 3.8 and 3.4).

In this section, all groups will be written additively and assumed to be abelian.

Definition 3.4. A *p-group* is a group of order p^n for some prime p and with $n \geq 1$.

Definition 3.5. Let A be an abelian group and let p be prime. We will let $A(p)$ denote the set of all elements of A whose order is a power of p.

Theorem 3.6 (Cauchy's Theorem). *If G is a finite commutative group whose order is divisible by a prime p, G contains an element of order p.*

Proof. Suppose that the only subgroups of G are $\{e\}$ and G itself. Then there exists some non-trivial element a such that $\langle a\rangle = G$, and $|a| = p$ as desired. Thus, G contains at least one proper subgroup. Assume by induction that if p divides the order of a subgroup

$K \subsetneq G$ (Note that $|K| < |G|$ necessarily), there exists an element $b \in H$ with $|b| = p$. Now, if there exists some nontrivial subgroup $H \subsetneq G$, $|G| = |G/H| \cdot |H|$ by Lagrange. This results in the following two cases:

Case 1: *p divides $|H|$.*

Since $|H| < |G|$, Then by our inductive hypothesis, there exists an element $b \in H$ of order p. Since $b \in H$, $b \in G$.

Case 2: *p divides $|G/H|$ and p doesn't divide $|H|$.*

By the same inductive hypothesis stated above, for $g \notin H$ we can find $gH \in G/H$ such that $H = (gH)^p = g^p H$. Then there must be an element $h_1 \in H$ such that $g^p h_1 = e$. Now, consider the map ϕ: $H \to H$ that maps $h \mapsto h^p$.

Claim. *ϕ is bijective.*

We first want to show that $h^p = k^p$ implies $h = k$. Indeed, $h^p = k^p$ does imply that $(hk^{-1})^p = e$. But then $|hk^{-1}|$ divides p, and so $|hk^{-1}| = 1$ or $|hk^{-1}| = p$. But if $|hk^{-1}| = p$, p divides H by Lagrange, which contradicts our assumption on H. So we have that $|hk^{-1}| = 1$, and so h is the unique inverse of k^{-1}, i.e., $h = k$ as desired. Thus, ϕ is injective. Since $|H|$ is finite and ϕ is 1-1, ϕ is onto as well, and we have that ϕ is bijective.

Since ϕ is onto, we can find an element $h_2 \in H$ such that $h_1 = h_2{}^p$. Then $b = gh_2$ satisfies $b^p = (gh_2)^p = g^p h_2{}^p = g^p h_1 = e$. Now, $|b| = 1$ implies $g \in H$, a contradiction. Therefore, we have that $|b| = p$. □

Proposition 3.7. *For any prime p, $A(p)$ is a subgroup of A. Moreover, if $A(p)$ is finite, $A(p)$ is a p-group.*

Proof. We first notice that $A(p)$ is non-empty as e has order p^0. If $|a| = p^{r_1}$ and $|b| = p^{r_2}$, $|ab|$ divides $|p^{r_1 r_2}|$, implying that $|ab|$ is a power of p. It is clear that $a^{-1} \in A(p)$ since $|a| = |a^{-1}|$. Therefore, by the two-step subgroup test $A(p)$ is a subgroup of A.

Now, suppose that $A(p)$ is finite and not a p-group, that is, that the order of $A(p)$ is $|A(p)| = p^r m$ where $\gcd(p, m) = 1$. If a prime $q \mid m$ then by Cauchy's Theorem above, $A(p)$ has some element of order q. But by definition, the order of every element $A(p)$ is a power of p. Thus, we have arrived at a contradiction, and the order of $A(p)$ must be p^k for some $k \leq r$, and thus $A(p)$ is a p-group. □

Definition 3.8. Let $B_1, B_2, \ldots, B_n$ be subgroups of an abelian group A. Then we denote the *direct sum* of these subgroups as $A = B_1 \oplus B_2 \oplus \cdots \oplus B_n$ if:

1. $A = B_1 + B_2 + \cdots + B_n = \{b_1 + b_2 + \cdots + b_n \mid b_i \in B_i\}$.
2. $(B_1 \oplus \cdots \oplus B_i) \cap B_{i+1} = \{0\}$ for all $1 \leq i \leq n-1$.

Note: An element in the direct sum is zero if and only if the components are all zero, shown as follows: If $0 = m_1a_1 + \cdots + m_ka_k \in A_1 \oplus \cdots \oplus A_k$ and $m_ka_k \neq 0$, then we have that $-m_ka_k = m_1a_1 + m_2a_2 + \cdots + m_{k-1}a_{k-1}$, and so $A_1 \oplus A_2 \oplus \cdots \oplus A_{k-1} \cap A_k \neq \{0\}$, a contradiction. Therefore m_k is 0. Continuing by induction, all $m_i = 0$.

Definition 3.9. An *exponent* of a group is any integer that annihilates that every element in the group.

Note, if G has exponent n, then G also has exponent kn where k is a positive integer.

Example 3.10. $\mathbb{Z}_n$ has exponent $n, 2n, 3n, \ldots$ On the other hand, $\mathbb{Z}$ does not have an exponent.

Example 3.11. $\mathbb{Z}_n[x]$, regarded as an infinite abelian group, has exponent $n, 2n, 3n, \ldots$

Theorem 3.12. *Let A be a finite abelian group. Then A is the direct sum of its subgroups $A(p)$ for all primes p for which $A(p) \neq \{0\}$.*

Proof. Consider a finite abelian group A with exponent n. We can write $n = mm'$ where $\gcd(m, m') = 1$. Then there exist integers r, s such that $1 = rm + sm'$. Then, for $a \in A, a = arm + asm' = mra + m'sa = ma' + m'a''$ where $a', a'' \in A$. Thus, $A \subseteq mA + m'A$. But as $mA \subseteq A$ and $m'A \subseteq A, mA + m'A \subseteq A$, and so $A = mA + m'A$.

Now, we consider an element b such that $b \in mA \cap m'A$. Then $b = ma_1 = m'a_2$ for some $a_1, a_2 \in A$. Thus, $mb = mm'a_2 = na_2 = 0$, and similarly $m'b = 0$. Therefore, $b = b \cdot 1 = rmb + sm'b = 0$, and so $A = mA \oplus m'A$.

We will now let $A_m = \{a \in A \mid ma = 0\}$ and $A_{m'} = \{a \in A \mid m'a = 0\}$. Taking $m'a \in m'A$, we have $mm'a = na = 0$, so $m'a \in A_m$. Similarly, $ma \in A_{m'}$. Conversely, if we take an element $b \in A_m, b = b \cdot 1 = brm + bsm' = rmb + m'sb$, and thus $b = m'sb = m'a \in m'A$. Therefore, $m'A = A_m$, and similarly $mA = A_{m'}$, which means $A = A_m \oplus A_{m'}$.

Write $n = p_1^{e_1} \cdots p_k^{e_k}$, a prime power decomposition with $p_i = p_j$ implying $i = j$. Assume $A_{p_1^{e_1}} \neq \{0\}$. Then $A = A_{p_1^{e_1}} \oplus A_q$ where $n = p_1^{e_1} q$ (an exponent of A). We will use induction on order. That is, whenever B is a finite abelian group with $|B| < |A|$ and having an exponent $q_1^{f_1} \cdots q_j^{f_j}$, then $B = B_{q_1^{f_1}} \oplus \cdots \oplus B_{q_j^{f_j}}$. The base case is left to the reader. Since $|A_q| < |A|$ and q is an exponent for A_q, $A_q = A_{p_2^{e_2}} \oplus \cdots \oplus A_{p_k^{e_k}}$ and therefore, $A = \bigoplus_{i=1}^{k} A_{p_i^{e_i}}$. Moreover, $A_{p_i^{e_i}} \neq \{0\}$.

Finally, we must show that $A_{p_i^{e_i}} = A(p_i)$. Let $a \in A_{p_i^{e_i}}$. Then $p_i^{e_i} a = 0$ implies that $|a|$ divides $p_i^{e_i}$, thus $|a|$ is a power of p_i, that is, $A_{p_i^{e_i}} \subseteq A(p_i)$. Now, as $|a|$ is a power of p_i, $|a| = p_i^t$ for some positive integer t. Since n is an exponent for A, p_i^t divides n. But then p_i^t divides $p_i^{e_i}$, so $p_i^{e_i} a = 0$, i.e., $A(p_i) \subseteq A_{p_i^{e_i}}$. Therefore, $A_{p_i^{e_i}} = A(p_i)$, and A can be written as follows:

$$A = \bigoplus_{i=1}^{k} A(p_i) \text{ with each } A(p_i) \neq \{0\}.$$

□

Example 3.13. Consider an abelian group A of order $36 = 2^2 \cdot 3^2$. Then $A(2)$ consists of all elements of orders $1, 2$, and 2^2 and $A(3)$ consists of those of orders $1, 3$, and 3^2. Thus, by Theorem 3.12 $A = A(2) \oplus A(3)$.

Lemma 3.14. *Let A be an abelian group. Consider $b \in A$ with $b \neq 0$, and let k be a positive integer such that $p^k b \neq 0$. If $|p^k b| = p^m$, then $|b| = p^{m+k}$.*

Proof. Since $p^m(p^k b) = p^{m+k} b = 0$, $|b|$ divides p^{m+k}. This implies that $|b| = p^{m+k-i}$ for $0 \leq i \leq p + m$. But $0 = p^{m+k-i} b = p^{m-i}(p^k b)$ implies p^m divides p^{m-i}, which can only happen if $i = 0$, that is, if $|b| = p^{m+k}$. □

Lemma 3.15. *Consider a finite abelian, non-cyclic p-group A, and let $a_1 \in A$ be an element of maximal order p^{r_1}. Consider $A_1 = \langle a_1 \rangle \subsetneq A$ and the quotient A/A_1. Let $\overline{b} = a + A_1 \in A/A_1$ be an element of order p^r. Then there exists a representative a of $\overline{b}$ with order p^r.*

Proof. Let b be any representative for $\overline{b}$. We note that since the order of the image of an element divides the order of the element and because the natural map $\phi\colon A \to A/A_1$ from $x \mapsto \overline{x}$ is a surjective homomorphism, $p^r = |\overline{b}| \leq |b|$. If we suppose $p^r b = 0$, then $|b| \leq p^r$, and we have that $|b| = p^r$ as desired. Consequently, we can assume that $p^r b \neq 0$.

Since $p^r\overline{b} = \overline{0}$, $p^r b + A_1 = 0 + A_1$, so $p^r b \in A_1$. Therefore, $p^r b = na_1$ for some $n \geq 0$. We can write $n = p^k\mu$ with $\gcd(p, \mu) = 1$. Then $p^r b = p^k \mu a_1$.

We will show that $|a_1| = |\mu a_1|$. Since $p^{r_1} = |a_1|$ annihilates a_1 and thus μa_1, we have that $|\mu a_1|$ divides $|a_1|$. Therefore, $|\mu a_1| = p^j$ for some $1 \leq j \leq r_1$, so $p^j(\mu a_1) = 0$. But $(p^j\mu)a_1 = 0$ implies that $p^{r_1} \mid p^j\mu$. Hence, $p^{r_1} \mid p^j$, implying $p^{r_1} = p^j$, and therefore $|a_1| = |\mu a_1|$. We can thus conclude that $|p^k \mu a_1| = p^{r_1 - k}$ with $k \leq r_1$.

Now, we have $p^r b \neq 0$, and $|p^k \mu a_1| = |p^r b| = p^{r_1 - k}$, so by Lemma 3.14, $|b| = p^{r_1 - k + r}$. As $p^{r_1}/$ is a maximal order for elements of A, $p^{r + r_1 - k} \leq p^{r_1}$, and thus $r + r_1 - k \leq r_1$, so $r \leq k$. We write $k = r + t$ where $0 \leq t \leq k$. Then, $p^r b = p^k \mu a_1 = p^{r+t}\mu a_1 = p^r(p^t \mu a_1)$, and if we write $c = p^t \mu a_1$, we have $p^r b = p^r c$ with $c \in A_1$.

Consider $a = b - c$. Then $\overline{a} = \overline{b - c} = \overline{b} - \overline{c} = \overline{b} + \overline{0} = \overline{b}$, and a is a representative for $\overline{b}$. Furthermore, $p^r b = p^r c$, and so $p^r(b - c) = 0$, which implies that $p^r a = 0$, and so $|a| \leq p^r = |\overline{a}|$. Additionally, by the first paragraph above $|\overline{a}| \leq |a|$, and thus $p^r = |\overline{a}| = |a|$. □

Theorem 3.16. *Every finite abelian p-group is isomorphic to a direct sum of cyclic p-groups. Moreover, this direct sum is unique up to reordering the factors.*

Proof. Let A be a p-group and let $a_1 \in A$ be an element of maximal order. If A is cyclic, there is nothing to show. Therefore, we can assume that A is not cyclic. Let $A_1 = \langle a_1 \rangle \subsetneq A$ with $|a_1| = p^{r_1}$. Now, consider A/A_1 with order less than $|A|$. Then by Lagrange, A/A_1 is a p-group of lesser order than A. By induction, we assume $A/A_1 = B_2 \oplus \cdots \oplus B_s$ where each B_i is a cyclic subgroup of A/A_1 of order p^{r_i} with $2 \leq i \leq s$.

Let $\overline{a_i} = a_i' + A_1$ be a generator for each B_i. By Lemma 3.15, we can find a representative $a_i \in A$ of each $\overline{a_i}$ having order p^{r_i} where $2 \leq i \leq s$. Suppose $A_i = \langle a_i \rangle \subseteq A$ for $2 \leq i \leq s$.

Claim. $A = A_1 \oplus A_2 \oplus \cdots \oplus A_s$.

We must first show that $A = A_1 + A_2 + \cdots + A_s$. It is clear that $A \supseteq A_1 + A_2 + \cdots + A_s$. To show $A \subseteq A_1 + A_2 + \cdots + A_s$, we take $x \in A$ and consider $\overline{x} \in A/A_1$. By our induction hypothesis, $A/A_1 = B_2 \oplus \cdots \oplus B_s$, so $\overline{x} = m_2\overline{a_2} + \cdots + m_s\overline{a_s} = \overline{m_2 a_2 + \cdots + m_s a_s}$ for representatives a_i of $\overline{a_i}$. Therefore, $x - (m_2 a_2 + \cdots + m_s a_s) \in A_1 = \langle a_1 \rangle$. Thus, $x - (m_2 a_2 + \cdots + m_s a_s) = m_1 a_1$, for some m_1 and so $x = m_1 a_1 + m_2 a_2 + \cdots + m_s a_s$, that is, $A \subseteq A_1 + A_2 + \cdots + A_s$, and therefore $A = A_1 + A_2 + \cdots + A_s$.

We now show that $(A_1 + \cdots + A_i) \cap A_{i+1} = \{0\}$ for all $i = 1, \ldots, s-1$. Suppose there are $m_1, \ldots, m_s \geq 0$ such that $m_1 a_1 + \cdots + m_s a_s = 0$.

Claim. *$m_i = 0$ for all i.*

We can assume that $m_i \leq p^{r_i}$. Applying the natural homomorphism $\phi\colon A \to A/A_1$ to $m_1 a_1 + \cdots + m_s a_s = 0$, we have $m_1\overline{a_1} + \cdots + m_s\overline{a_s} = \overline{0}$. Now, as $\overline{0} = m_1\overline{a_1} + \cdots + m_s\overline{a_s} \in B_2 \oplus \cdots \oplus B_s$, $m_i = 0$ for $2 \leq i \leq s$. But then, we have $m_1 a_1 = 0$, implying that $m_1 = 0$, so $m_i = 0$ for all i such that $0 \leq i \leq s$.

Finally, $y \in A_{i+1} \cap \sum_{j=1}^{i} A_j$ implies $m_{i+1}a_{i+1} = y = \sum_{j=1}^{i} m_j a_j$ for some m_j. Since $y - y = 0$, we have that $m_j = 0$ for all $j, 0 \leq j \leq i+1$. Therefore, $A = A_1 \oplus \cdots \oplus A_s$, a direct sum of cyclic p-groups by Definition 3.8. Uniqueness of this direct sum decomposition can also be shown to hold (See Lang p. 48). □

Example 3.17. Recall our abelian group of order 36 with $A = A(2) \oplus A(3)$ from Example 3.13. Then by Theorem 3.16, $A(2)$ decomposes as $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $A(3)$ breaks down as $\mathbb{Z}_9$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. This leaves us with 4 potential decompositions for A:

1. $A = \mathbb{Z}_4 \oplus \mathbb{Z}_9$.
2. $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$.
3. $A = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$.
4. $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

3.3 Finitely Generated Abelian Groups

The last major result we will need before proceeding to Ore's Theorem is the Fundamental Theorem of Finitely Generated Abelian Groups (see Theorem 3.28) as well as associated definitions and results. Like the major results of the previous section, the Fundamental Theorem of Finitely Generated Abelian Groups details the direct sum decomposition of finitely generated abelian groups.

Definition 3.18. If a, b are any two elements of an abelian group A, then for scalars $\alpha, \beta \in \mathbb{Z}$ the element $\alpha a + \beta b$ is called a *linear combination* of a and b in A. This definition extends similarly for any finite number of elements. A collection of elements

of A is *linearly independent* if whenever a linear combination of elements equals zero, all the scalars equal zero.

Definition 3.19. An abelian group has a *basis* if there exists a subset of linearly independent elements with which every element of the group can be written as a linear combination.

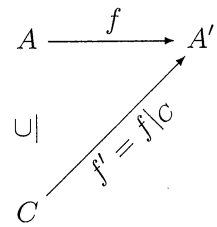
Definition 3.20. An abelian group A is called *free* if it has a basis.

Example 3.21. Any direct sum $\oplus_I \mathbb{Z}$ is an abelian group; moreover, it has a basis (standard basis) consisting of the functions $e_i \colon I \to \mathbb{Z}$ whose value at j is zero if $j \neq i$ and 1 if $j = i$ where $i, j \in I$. Therefore $\oplus_I \mathbb{Z}$ is free.

Lemma 3.22. *Let $f \colon A \to A'$ be a surjective homomorphism of abelian groups where A' is free, and let B be the kernel of f. Then*

1. *There exists a subgroup C of A such that f restricted to C induces an isomorphism with A'.*
2. *$A = B \oplus C$.*

Proof. We may visualize assertion 1 with the diagram pictured below.



1. Because A' is free abelian by hypothesis, it has a basis, $\{x'_i : i \in I\}$. Additionally, as f is surjective, each x'_i has a preimage $x_i \in A$ such that $f(x_i) = x'_i$. Let $C = \langle X \rangle$, the subgroup generated by $X = \{x_i : i \in I\}$ in A. We will consider the restriction of f to C, denoted by $f' = f|_C$.

   Claim. *$f' \colon C \to A'$ is an isomporphism.*

We know that f' is a homomorphism because it is a restriction of f, which is itself a homomorphism. Thus, we need only show that f' is bijective. To show that f' is surjective, we consider $a' \in A'$. Because A' is free, we can write $a' = \sum \alpha_i x_i'$ where $\alpha_i \in \mathbb{Z}$. Then the element $a \in C$ given by $a = \sum \alpha_j x_j$ satisfies $f'(\sum \alpha_j x_j) = \sum \alpha_j f'(x_j) = \sum \alpha_j x_j' = a'$. Thus, f' is onto.

We now show that f' is injective. Let $c \in C$ with $f'(c) = 0$. Then $c \in \langle X \rangle$, which implies that there exists a $J \subseteq I$ that is finite and scalars $\alpha_j \in \mathbb{Z}$ such that $c = \sum_J \alpha_j x_j$. Then $0 = f'(c) = f'(\sum \alpha_j x_j) = \sum \alpha_j f'(x_j) = \sum \alpha_j x_j'$. Since the $x_j's$ are a basis each $\alpha_j = 0$ and thus $c = 0$. Therefore, f' is injective, and thus $f' \colon C \to A'$ is an isomorphism.

2. To show $A = B \oplus C$, we must show that $B \cap C = \{0\}$, and that $A = B + C$. If we take $x \in B \cap C, f(x) = 0$ since $B = \ker f$. But since $x \in C, f(x) = f'(x)$. As f' is injective, $x = 0$ and thus $B \cap C = \{0\}$. If we take $a \in A, f(a) \in A'$. So $f(a) = \sum \alpha_j x_j'$. for some scalars α_j. If we take $c = \sum \alpha_j x_j \in C$, consider $a - c$. Applying f, we have $f(a - c) = f(a) - f(c) = f(a) - f(\sum \alpha_j x_j) = f(a) - \sum \alpha_j f(x_j) = f(a) - \sum \alpha_j x_j' = f(a) - f(a) = 0$. Thus, $a - c \in B$, i.e., $a - c = b$, and so, $a = b + c$ as desired. Therefore, $A = B \oplus C$. □

Theorem 3.23. *Let B be a subgroup of a finitely generated free abelian group A. Then B is a free abelian group itself on a basis with cardinality less than or equal to the cardinality of a basis for A.*

Proof. Suppose A has n generators, $A \cong \overset{n}{\underset{1}{\oplus}} \mathbb{Z}_i, (\mathbb{Z}_i = \mathbb{Z})$. We proceed by induction on n. If A is free on one generator, that is, $A \cong \mathbb{Z}$, then $B \subseteq A$ is either free on zero generators, that is, either $B = \{0\}$, or since every non-zero subgroup of $\mathbb{Z}$ is infinite cyclic, B is infinite cyclic and therefore free on one generator.

Now we assume that the theorem is true for any group with fewer than n generators. Consider the surjective projection homomorphism $\pi \colon A \to \mathbb{Z}_1$ that sends $(x_1, \ldots, x_n) \mapsto x_1$.

We note that $\ker \pi \cong \overset{n}{\underset{2}{\oplus}} \mathbb{Z}_i$, which we regard as an identification. We define $B_1 = B \cap \ker \pi = \ker \pi|_B$. Thus, $B_1 \subseteq \overset{n}{\underset{2}{\oplus}} \mathbb{Z}_i$, and is free on less than $n - 1$ generators by the induction hypothesis. Now, we consider the direct image of B under $\pi, \pi(B) = \pi|_B(B) \subseteq \mathbb{Z}_1$. We have the following two cases:

Case 1: $\pi(B) = \{0\}$.

If $\pi(B) = \pi|_B(B) = \{0\}$, then $B = \ker \pi|_B$. But as $\ker \pi|_B = B_1, B = B_1$ is free on $\leq n-1$ generators.

Case 2: $\pi(B) \neq \{0\}$.

If $\pi(B) \neq \{0\}$, then $\pi(B)$ is a non-zero subgroup of $\mathbb{Z}$, and is therefore infinite cyclic. Thus, $\pi(B) \cong \mathbb{Z}$, and as $\mathbb{Z}$ is free on one generator, $\pi(B)$ free on one generator. Now, as $\pi|_B$ is onto it's image, there exists a subgroup C of B by Lemma 3.22 such that $B = C \oplus \ker \pi|_B$ with $C \cong \pi|_B(B)$. Thus, C is free on one generator, and B_1 is free on $\leq n-1$ generators, and therefore B is free on $\leq n$ generators. □

Definition 3.24. A *torsion element* of an abelian group is any non-zero element with finite order. If a group has no torsion elements it is called *torsion-free.*

Example 3.25. Every element of $\mathbb{Z}_n$ (integers modulo n) is a torsion element. $\mathbb{Q}/\mathbb{Z}$ is an infinite group whose elements are all torsion. Note: $\oplus_I \mathbb{Z}$ (where I is any index set) is torsion free.

Note: $\bigoplus_{i=1}^{n} \mathbb{Z}$ is the typical case of a finitely generated torsion-free abelian group as the following theorem (Theorem 3.26) shows.

Theorem 3.26. *If A is a finitely generated torsion-free abelian group, then A is free.*

Proof. Assume $A \neq \{0\}$, and let S be a finite set of generators of A. Suppose $X = \{x_1, \ldots, x_n\}$ is a maximal linearly independent subset of S. If B is the subgroup generated by X, then B is free by definition.

By maximality on X, given any $z \in S$, there exist integers $m_1, \ldots, m_n$ not all equal to zero and $\mu \neq 0$ such that $\mu z + m_1 x_1 + \cdots + m_n x_n = 0$. Therefore, $\mu z \in B$. Thus, we note that we can find such a μ_i with $\mu_i z_i \in B$ for each of the finitely many elements of S. Supposing there are k generators of A, we take $m = \mu_1 \mu_2 \cdots \mu_k$. Now, given $y \in A$, i.e., $y = \sum \alpha_i z_i (z_i \in S, \alpha_i \in \mathbb{Z}), my = \sum \alpha_i (m z_i) \in B$. As this m is independent of the choice of $y \in A, mA \subseteq B$.

Now, we consider the homomorphism $\phi\colon A \to mA$ that sends x to mx. Furthermore, because A is torsion-free, $\ker \phi = \{0\}$, and thus our map is also one to one, and therefore an isomorphism of A onto $mA \subseteq B$, a subgroup. Therefore, we can conclude by Theorem 3.23 that mA is free, and so A is free. □

Lemma 3.27. *Let A be an abelian group. Then A_T, the set of all torsion elements of A, forms a subgroup of A.*

Proof. We note that A_T is non-empty as $e \in A_T$. Suppose $a, b \in A_T$ with $a^m = e$ and $b^n = e$. Then $(a^{-1})^m = (a^m)^{-1} = (e)^{-1} = e$, so $a^{-1} \in A_T$. Furthermore, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = ee = e$. Thus, $ab \in A_T$, and by the two-step subgroup test, A_T is a subgroup of A. □

Theorem 3.28 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let A be a finitely generated abelian group, and let A_T be the subgroup of all torsion elements of A. Then*

1. *A_T is finite.*
2. *A/A_T is free.*
3. *There exists a subgroup $B \subseteq A$ such that B is free and $A = A_T \oplus B$.*

Proof.

1. If $a \in A_T$, there exist scalars $\alpha_i \in \mathbb{Z}$ such that $a = \sum_{i=1}^{n} \alpha_i x_i$. Since there are finitely many generators and finitely many distinct scalars α_i modulo $|x_i|$ such that $\alpha_i x_i \neq 0$, there are finitely many elements in A_T, and so A_T is finite.
2. We begin by showing A/A_T is torsion-free. Let $X = \{z_1, \ldots, z_n\}$, one for each generator x_i of A, be a basis for the free abelian group F on X whose elements have the form $\sum_{i=1}^{n} \alpha_i z_i$ where $\alpha_i \in \mathbb{Z}$. By the Universal Mapping Property there exists a unique homomorphism $\phi\colon F \to A$ such that $\phi(\sum \alpha_i z_i) = \sum \alpha_i x_i$. Note that ϕ is onto A.

   Considering just the torsion elements A_T of A, the inverse image of A_T under ϕ is a subgroup of F. Since F is free on n generators, $\phi^{-1}(A_T)$ is free on $\leq n$ generators by Theorem 3.23. Additionally, as ϕ is onto A, ϕ is onto A_T, and so $\phi(\phi^{-1}(A_T)) = A_T$. Because $\phi^{-1}(A_T)$ is finitely generated, $\phi(\phi^{-1}(A_T))$ is finitely generated as well. So $A_T = \phi(\phi^{-1}(A_T))$ is finitely generated and abelian.

   We now consider A/A_T. Suppose $\overline{x} = x + A_T$ has finite period m. Then $m\overline{x} = \overline{0} \in A/A_T$. Then $m(x + A_T) = mx + A_T = 0 + A_T$, implying $mx \in A_T$. Since mx is a torsion element, there exists a $q \neq 0$ such that $q(mx) = 0$ in A. Then $(qm)x = 0$ so $x \in A_T$. But $x \in A_T$ implies $\overline{x} = \overline{0} \in A/A_T$. Thus, there are no non-zero elements of A/A_T with finite period, i.e., A/A_T is torsion-free. Therefore, by Theorem 3.26, A/A_T is free.

3. Consider the natural surjective homomorphism $f\colon A \to A/A_T$, which sends $x \mapsto x + A_T$. Then $\ker f = A_T$. By Lemma 3.22, there exists a subgroup B of A such that $f|_B\colon B \to A/A_T$ is an isomorphism. Thus, B is free, and $A = B \oplus A_T$.

□

Chapter 4

Ore's Theorem

With the structures of finite abelian and finitely generated abelian groups in hand, we are prepared to prove Ore's Theorem. Before proceeding to Ore's Theorem, however, we need the following definition and lemmas. Note that in this section all groups are written multiplicatively. $\mathcal{C}_n$ will denote a cyclic group of order n and $\mathcal{C}_\infty$ will denote an infinite cyclic group. Note: $\mathcal{C}_n \cong \mathbb{Z}_n$, and $\mathcal{C}_\infty \cong \mathbb{Z}$. Also, when written mutliplicatively, direct sum is refered to as direct product and defined in an analogous manner.

Definition 4.1. For any group G, $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$ is called the *center* of G. Note that $Z(G)$ is always a subgroup of G.

Lemma 4.2. *Let H be a subgroup of G, and let $H \subseteq Z(G)$. Then $H \trianglelefteq G$. Furthermore, if G/H is cyclic, then G is abelian.*

Proof. First, we show $H \trianglelefteq G$. By the normal subgroup test, it suffices to show that $g^{-1}hg \in H$. But since $h \in Z(G), g^{-1}hg = g^{-1}gh = h \in H$, so H is normal.

Next, we assume that $G/H = \langle gH \rangle$ is cyclic. Consider elements $g_1, g_2 \in G$. Then $g_1H = g^iH$, thus $g_1 = g^ih_1$ for some $h_1 \in H$. Similarly, $g_2 = g^jh_2$ for some $h_2 \in H$. Then we have $g_1g_2 = g^ih_1g^jh_2 = g^ig^jh_1h_2 = g^{i+j}h_1h_2 = g^{j+i}h_1h_2 = g^jg^ih_1h_2 = g^jg^ih_2h_1 = g^jh_2g^ih_1 = g_2g_1$ since $h_1, h_2 \in Z(G)$. Therefore, G is abelian. □

Definition 4.3. A group is *locally cyclic* if every finite number of elements generates a cyclic subgroup.

Note that every cyclic group is locally cyclic because every subgroup of a cyclic group is cyclic. The converse, however, is not true as illustrated by the following example.

Example 4.4. Consider the group of rational numbers under addition and note that any two elements a/b and c/d in $\mathbb{Q}$ are contained in the cyclic subgroup generated by $1/bd$. Therefore, although $\mathbb{Q}$ is clearly not cyclic, it is locally cyclic.

Lemma 4.5. *Every locally cyclic group is abelian.*

Proof. Let G be a locally cyclic group. Taking any elements x and y of G, $\langle x, y\rangle = \langle g\rangle$ for some $g \in G$. Then $x = g^m$ and $y = g^n$, and thus $xy = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = yx$. □

Theorem 4.6 (Ore's Theorem). *Given a group G, $\mathrm{Sub}(G)$ is distributive if and only if G is locally cyclic.*

Proof. We begin by assuming that $\mathrm{Sub}(G)$ is distributive. Consider $a, b \in G$. First, we will show that the subgroup generated by a and b, denoted $\langle a, b\rangle$, is cyclic. Recall that that we form the meet of two subgroups by taking the subgroup generated by those subgroups. Hence, $\langle ab\rangle \vee \langle a\rangle$ is the subgroup generated by $\langle ab\rangle$ and $\langle a\rangle$. We want to show that $\langle ab\rangle \vee \langle a\rangle = \langle a, b\rangle$. It is clear that the subgroups generated by $\langle ab\rangle$ and $\langle a\rangle$ are each seperately contained in the subgroup generated by $\langle a, b\rangle$, and so $\langle ab\rangle \vee \langle a\rangle \subseteq \langle a, b\rangle$. To show that $\langle a, b\rangle \subseteq \langle ab\rangle \vee \langle a\rangle$, we need only show the generators of $\langle a, b\rangle$ are in the set $\langle ab\rangle \cup \langle a\rangle$. We have that $a \in \langle ab\rangle \cup \langle a\rangle$ by closure. As both a and $ab \in \langle ab\rangle \cup \langle a\rangle$, $a^{-1}ab = b \in \langle ab\rangle \cup \langle a\rangle$ as well. So $\langle a, b\rangle \subseteq \langle ab\rangle \vee \langle a\rangle$ and by double inclusion $\langle ab\rangle \vee \langle a\rangle = \langle a, b\rangle$. We can similarly show that $\langle ab\rangle \vee \langle b\rangle = \langle a, b\rangle$.

Now, since $\mathrm{Sub}(G)$ is distributive, $\langle ab\rangle \vee (\langle a\rangle \wedge \langle b\rangle) = (\langle ab\rangle \vee \langle a\rangle) \wedge (\langle ab\rangle \vee \langle b\rangle)$. But since $\langle ab\rangle \vee \langle a\rangle = \langle a, b\rangle = \langle ab\rangle \vee \langle b\rangle$, we have that $\langle ab\rangle \vee (\langle a\rangle \wedge \langle b\rangle) = \langle a, b\rangle$. It is important to note that a and b commute with all the elements of $\langle a\rangle \wedge \langle b\rangle$ as follows: Given $c \in \langle a\rangle \wedge \langle b\rangle$, c has the form $c = a^k$ and $c = b^j$. Then $ac = aa^k = a^{1+k} = a^{k+1} = a^k a = ca$. Similarly, $bc = bb^j = b^{1+j} = b^{j+1} = b^j b = cb$. Therefore, $\langle a\rangle \wedge \langle b\rangle \subseteq Z(\langle a, b\rangle)$. Hence, by Lemma 4.2 above, $\langle a\rangle \wedge \langle b\rangle \trianglelefteq \langle a, b\rangle$, and so by the 2nd Isomorphism Theorem for Groups (Theorem 3.3),

$$\langle a, b\rangle / (\langle a\rangle \wedge \langle b\rangle) \cong \langle ab\rangle / \langle ab\rangle \wedge (\langle a\rangle \wedge \langle b\rangle). \tag{4.1}$$

We note that $\langle a, b\rangle / (\langle a\rangle \wedge \langle b\rangle)$ is cyclic since a quotient of cyclic groups is cyclic, and so Lemma 4.2 implies that $\langle a, b\rangle$ is abelian. Therefore, the Fundamental Theorem

of Finitely Generated Abelian Groups (Theorem 3.28) applies, and $\langle a, b\rangle$ decomposes as $\langle a, b\rangle = \langle a, b\rangle_T \times F$, the direct product of respective torsion and free subgroups of $\langle a, b\rangle$. This decomposition yields the following three cases:

Case 1: $\langle a, b\rangle_T = \{0\}$.

If $\langle a, b\rangle$ has no torsion elements, it is a free group on 2 generators and is thus isomorphic to $\mathcal{C}_\infty \times \mathcal{C}_\infty$.

Case 2: $\langle a, b\rangle_T$ *has one generator.*

If $\langle a, b\rangle_T$ has one generator, F is free on ≤ 1 generator by Theorem 3.23. Then $\langle a, b\rangle_T \cong \mathcal{C}_n$ and $F \cong \mathcal{C}_\infty$ or $F = \{0\}$. Thus, $\langle a, b\rangle = \mathcal{C}_n$ or $\langle a, b\rangle = \mathcal{C}_n \times \mathcal{C}_\infty$, a product of cyclic groups.

Case 3: $\langle a, b\rangle = \langle a, b\rangle_T$.

Because $\langle a, b\rangle$ is finite abelian, Theorem 3.16 applies, and $\langle a, b\rangle$ is a direct product of no more than 2 finite cyclic subgroups.

As we have shown above, $\langle a, b\rangle = \langle u\rangle \times \langle v\rangle$, a direct product of cyclic groups. This implies that $\langle u\rangle \wedge \langle v\rangle = \{e\}$, and so by display 4.1, $\langle u, v\rangle/(\langle u\rangle \wedge \langle v\rangle) = \langle u, v\rangle$ is cyclic. But $\langle a, b\rangle = \langle u\rangle \times \langle v\rangle = \langle u, v\rangle$, and so $\langle a, b\rangle$ is cyclic and thus G is locally cyclic.

For the converse, assume that G is locally cyclic, and let A, B, and C be subgroups of G. We want to show that $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$. By Proposition 2.25, $A \vee (B \wedge C) \subseteq (A \vee B) \wedge (A \vee C)$ is always true, and we need only show that $(A \vee B) \wedge (A \vee C) \subseteq A \vee (B \wedge C)$. Because G is locally cyclic, G is commutative and therefore every subgroup is normal. Since the meet of any two subgroups is the intersection of those subgroups and the join of two normal subgroups can be formed by taking the product of those subgroups, it suffices to show that $AB \cap AC \subseteq A(B \cap C)$.

We take $x \in AB \cap AC$. Then $x = ab$ and $x = a'c$ for some $a, a' \in A, b \in B$ and $c \in C$. Because G is locally cyclic, $\langle a, a', b, c\rangle = \langle g\rangle$ for some $g \in G$. Let $A' = A \cap \langle g\rangle, B' = B \cap \langle g\rangle$, and $C' = C \cap \langle g\rangle$.

Claim. $\langle g\rangle = A'B'$ *and* $\langle g\rangle = A'C'$.

It is clear that $A'B' \subseteq \langle g\rangle$ and $A'C' \subseteq \langle g\rangle$. To show $\langle g\rangle \subseteq A'B'$, we need only show that the generators a, a', b and c of $\langle g\rangle$ are in $A'B'$. Note that $a, a' \in A'B'$ and $b \in A'B'$. Because $a'c = ab, c = a'^{-1}ab \in A'B'$ as well, and so $\langle g\rangle \subseteq A'B'$. Similarly, $\langle g\rangle \subseteq A'C'$. Notice that if $A' = \{e\}, a = e = a'$, and so $b = x = c$, and therefore

$x \in A(B \cap C)$. If either B' or $C' = \{e\}, x = a$ or $x = a'$, and thus $x \in A(B \cap C)$, and we are done. Therefore, we assume none of A', B' or C' are trivial.

Now, let $a = g^\alpha, a' = g^{\alpha'}, b = g^\beta$, and $c = g^\gamma$. Since $A'B' = \langle g \rangle$ we can find integers i and j such that $g = g^i g^j$ with $g^i \in A'$ and $g^j \in B'$, and hence $g^\gamma = g^{(i+j)\gamma}$. Now, $x = a'c = g^{\alpha'} g^{(i+j)\gamma} = g^{\alpha'} g^{i\gamma} g^{j\gamma}$. Then $g^{\alpha'} g^{i\gamma} \in A'$ and $g^{j\gamma} \in B' \cap C'$, and so $x \in A'(B' \cap C') \subseteq A(B \cap C)$. Therefore, Sub$(G)$ is distributive as desired. □

The following result follows immediately from Ore's Theorem and the definition of locally cyclic.

Corollary 4.7. *If G is a finite group,* Sub(G) *is distributive if and only if G is cyclic.*

Proof. Since every cyclic group is locally cyclic, if G is cyclic we have that G is distributive by Ore's Theorem. Conversely, if we assume that G is distributive, G is locally cyclic by Ore's Theorem. But because every finite number of elements generates a cyclic subgroup by the definition of locally cyclic and since G itself is a finite group, G itself must be cyclic. □

Definition 4.8. A poset satisfies the *ascending chain condition (ACC)* if every ascending chain of elements eventually terminates.

There are many mathematical structures that satisfy ACC.

Example 4.9. In any finite-dimensional vector space, every collection of subspaces satisfies ACC.

Example 4.10. In any principle ideal domain R, every collection of ideals satisfies ACC.

Theorem 4.11. *A group G is cyclic if and only if* Sub(G) *is distributive and satisfies the ascending chain condition.*

Proof. Suppose that G is cyclic. Then Sub(G) is distributive by Ore's Theorem, and we need only show that Sub(G) satisfies ACC. Since G is cyclic, let $G = \langle a \rangle$ for some $a \in G$. Then $\langle a^j \rangle \subseteq \langle a^k \rangle$ if and only if k is a divisor of j. This implies that every ascending chain in Sub(G) is finite, and thus terminates, and so Sub(G) satisifes ACC.

Conversely, assume Sub(G) is distributive and satisfies ACC. Let $\{a_1, a_2, \dots\}$ be a list of generators for G. Then the ascending sequence of subgroups $\langle a_1 \rangle, \langle a_1, a_2 \rangle, \dots$

must terminate at some step, say n. Thus, $a_{n+j} \in \langle a_1, \ldots, a_n \rangle$ for every $j \geq 0$. But then $\langle a_1, a_2, \ldots \rangle \subseteq \langle a_1, a_2, \ldots, a_n \rangle$, and so G is finitely generated. Additionally, G is locally cyclic by Ore's Theorem. Now, as G is finitely generated, Definition 4.3 implies that G is cyclic. $\square$

Chapter 5

Conclusion

In the introduction of this thesis, we asked a series of questions. First, we wondered if every conceivable lattice is isomorphic to the subgroup lattice of some group. Although we were able to find a class of groups whose subgroup lattices are isomorphic to the class of all finite lattice chains, for example, we found that there is no group whose subgroup lattice is isomorphic to the lattice N_5. However, Ph. Whitman was able to show that every lattice embeds as a sublattice in $\mathrm{Sub}(G)$ for some group G. This does not indicate that the lattice itself is a $\mathrm{Sub}(G')$ for some group G'.

Second, we wondered what kinds of lattice structures are isomorphic to which types of group structures. After a considerable amount of group theory involving the structure of finite abelian groups and finitely generated abelian groups, Ore's Theorem and its corollaries provide us with several results relating distributive lattices with cyclic groups. Specifically:

1. Given a group G, $\mathrm{Sub}(G)$ is distributive if and only if G is locally cyclic.
2. If G is a finite group, $\mathrm{Sub}(G)$ is distributive if and only if G is cyclic.
3. A group G is cyclic if and only if $\mathrm{Sub}(G)$ is distributive and satisfies the ascending chain condition.

In light of these results, we have a beautiful connection between two seemingly different subjects: group theory and lattice theory.

Bibliography

[D02] B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order*, second edition, Cambridge University Press, New York, 2002.

[Ga06] Gallian, J. *Contemporary Abstract Algebra*, sixth edition, Houghton Mifflin Company, Boston, 2006.

[Gr78] Gratzer, G.A. *General Lattice Theory*, first edition, Academic Press, Boston, 1978.

[L84] Lang, S. *Algebra*, second edition, Addison Wesley Publishing Company, Boston, 1984.

[S94] Schmidt, R. *Subgroup Lattices of Groups*, Expositions in Math., vol. 14, de Gruyter, New York, 1994.